



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/771,472	01/26/2001	Jean Louis Calvignac	RAL920000119US1	6208
25299	7590	04/21/2005	EXAMINER	
IBM CORPORATION PO BOX 12195 DEPT 9CCA, BLDG 002 RESEARCH TRIANGLE PARK, NC 27709			TRAN, ELLEN C	
			ART UNIT	PAPER NUMBER
			2134	

DATE MAILED: 04/21/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/771,472	Applicant(s) CALVIGNAC ET AL.	
	Examiner Ellen C Tran	Art Unit 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 01 December 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-8 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-8 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

Te

4

DETAILED ACTION

1. This action is responsive to communication: 1 December 2004, the original application was filed on 26 January 2001.
2. Claims 1-8 are currently pending in this application. Claim 1 is an independent claim.

Response to Arguments

3. Applicant's arguments with respect to claims 1-8 have been considered but are not persuasive.

In response to applicant's argument beginning on page 5, "However, there is no indication in Coppersmith that the cipher functions can be completed in a single hardware cycle regardless of whether a subprocess is embodied in a hardware chip". The Office disagrees Coppersmith clearly shows that the cipher can be completed in a single hardware cycle in col. 7, lines 5-10 "One or more of the subprocesses may be embodied in a hardware chip".

In response to applicant's argument on page 8, "it would be impossible to construct a hardware circuit with circuitry which would have to cycle only one for each encryption process". The Office disagrees with argument, as stated above Coppersmith clearly shows that the cipher can be completed in a hardware chip".

In response to applicant's argument on page 8, "Consequently, Coppersmith fails to disclose combinational logic performing computation iterations of a crypto-function on data stored in a first register and outputting data to a second register in a single hardware cycle, as set forth in Claim 1". The Office disagrees with argument. Coppersmith

Art Unit: 2134

discloses multiple combinational logic and that the one or more subprocesses can be embodied in hardware. This has the same meaning as the claimed invention.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language

5. **Claims 1-8** are rejected under 35 U.S.C. 102(e) as being anticipated by Coppersmith et al. U.S. Patent No. 6,189,095 (hereinafter ‘095).

As to independent claim 1, **“A hardware implementation of a crypto-function comprising”** is taught in ‘095 col. 5, lines 34-35 “Another object of the present invention is to provide a solution that can be implemented in hardware or software”;

“a first register storing data to be encrypted or decrypted; a second register for receiving data which has been encrypted or decrypted and combinational logic performing computation iterations of the crypto-function on data stored in the first register and outputting data to said second register” is shown in ‘095 col. 5, lines 41-67 “to provide a technique whereby the cipher used for encryption and decryption uses multiple stages, where each stage uses multiple Feistel network types that affect each word of the block”

“in a single hardware cycle” is disclosed in ‘095 col. 7, lines 10-11 “One or more of the subprocesses may be embodied in a hardware chip”.

As to dependent claim 2, **“wherein the crypto-function is a block cipher algorithm”** is taught in ‘095 col. 5, lines 20-21 “whereby encryption is accomplished using a symmetric key block cipher”.

As to dependent claim 3, **“wherein the crypto-function is the Data Encryption Standard (DES) algorithm”** is shown in ‘095 col. 6, lines 55-64 “network may be the inverse of the first modified Type-1 unbalanced Feistel network”.

As to dependent claim 4, **“wherein the crypto-function is the CHAIN algorithm”** is disclosed in ‘095 col. 6, lines 1-7 “variable information used by the algorithm--i.e., key length, block length, and number of rounds of expansion and number of stages can be factored into”.

As to dependent claim 5, **“wherein the combinational logic performs an invertible key-dependent round function iterated a predetermined number of times”** is taught in ‘095 col. 7, lines 2-10 “This modification may comprise applying a bitwise rotation to the input word in a plurality of selected rounds, applying a feedback operation using the input word”.

As to dependent claim 6, **“wherein the combination logic performs mixing, permutation and key-dependent substitution in each round”** is shown in ‘095 col. 6, lines 29-45 “the invention as broadly described herein, the present invention provides a technique, system, and method for implementing a symmetric key block cipher supporting variable length block, and a variable number of rounds of an expansion function, wherein the stages have a plurality of rounds, and rounds have a plurality of

Art Unit: 2134

subrounds, comprising : a subprocess for generating a plurality of subkeys using the input key and a first pseudorandom function”.

As to dependent claim 7, “wherein the combinational logic enciphers a block by performing an initial permutation of a block to be enciphered and then a complex key-dependent computation followed by a permutation which is an inverse of the initial permutation” is disclosed in ‘095 col. 7, lines 4-7 “applying a feedback operation using the input word in a plurality of the selected rounds, or both. The feedback preferably comprises an invertible function such as addition or exclusive OR”.

As to dependent claim 8, “wherein the combinational logic decipheres a block by performing deciphering using the same key as used to encipher the block in a process that is an inverse of the enciphering process” is taught in ‘095 col. 9, lines 45-51 “Decryption of data is accomplished in the present invention using the inverse of the data encryption, where the processes used for encryption are performed in reverse order”.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a). A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the

Art Unit: 2134

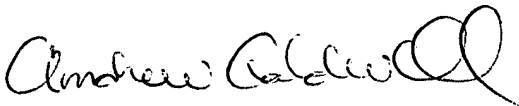
statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:30 am to 3:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ellen Tran
Patent Examiner
Technology Center 2134
12 April 2005


ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER